U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

January 26, 2024

BY ECF
The Honorable Lewis A. Kaplan
United States District Judge
Southern District of New York
500 Pearl Street
New York, NY 10007

Re: *United States v. Joseph Garrison*, 23 Cr. 597 (LAK)

Dear Judge Kaplan:

The Government respectfully submits this letter in advance of the January 29, 2024, sentencing of defendant Joseph Garrison. For the reasons set forth below, a sentence of a substantial term of imprisonment—at least 18 months—but less than the stipulated Guidelines range of 24 to 30 months' imprisonment (the "Stipulated Guidelines Range") is sufficient but not greater than necessary to serve the purposes of sentencing.

I. The Offense Conduct

A. The Attack

On November 18, 2022, hackers launched a "credential stuffing attack" (the "Attack") on a fantasy sports and sports betting website (the "Betting Website"). In the Attack, the hackers took large lists of stolen or leaked username and password combinations for other websites, and used computer programs to attempt to log into the Betting Website using those same username and password combinations. The hackers successfully accessed approximately 60,000 victim accounts at the Betting Website using those stolen username and password combinations.

The hackers also developed a method to steal funds in the victims' accounts, and used that method to steal a total of approximately $600,000 from approximately 1,600 accounts. The Betting Website made the individual victims whole, and incurred additional costs of approximately $700,000 to address and remediate the Attack.

The hackers who initially launched the Attack did not personally withdraw most of that $600,000 into their own accounts, in part because doing so would have made their detection much easier. Instead, individuals who commit credential stuffing attacks like the Attack frequently sell access to the stolen accounts they have obtained to online marketplaces that traffic in stolen accounts, among other things, and which are commonly referred to as "shops." In this case, the

hackers sold access to the stolen accounts[1] on shops they controlled and also sold access in bulk to other shops, which then sold access to stolen accounts on a retail level.

B. Garrison's Role in the Attack

Websites are designed to prevent these kinds of automated credential stuffing attacks through various means, including through the use of "Completely Automated Public Turing test to tell Computers and Humans Apart," or "CAPTCHAs." Successfully launching such an attack therefore requires a hacker to create a method that defeats the specific website's protections. Garrison was not the hacker who initially created the method used to attack the Betting Website, but he himself repeatedly used that method during the Attack to directly obtain stolen accounts from the Betting Website.

Once Garrison accessed accounts on the Betting Website, he sold that access in bulk to individuals who ran several other shops in exchange for a share of their profits. Garrison also created instructions for buyers to steal funds from victim accounts, and the instructions he created were used on a number of shops.

C. Garrison's Additional Hacking and Prior Police Contact

The Attack occurred on November 18, 2022. In or about June 2022—approximately five months before the Attack—he called in a bomb threat to his high school, PSR ¶ 54, and was subsequently interviewed by local police. Garrison told the police that he conducted credential stuffing attacks on websites and sold stolen accounts on a shop he controlled called "Goat Shop." Garrison said that he had been conducting such attacks from 2018 until 2021, that he made approximately $15,000 per day from selling stolen accounts at his peak, and that he made approximately $800,000 in total from his hacking. Garrison also told the police—falsely—that he had stopped hacking.

Messages and documents found on Garrison's electronic devices corroborate his involvement in a number of similar hacks. Law enforcement located files designed for use in credential stuffing attacks for dozens of corporate websites, and approximately 38 *million* sets of username and password combinations. Garrison told coconspirators:

- "Im getting sites no1 has had for like ever and shit. i have every captcha bypassed"
- "fraud is fun. im addicted to see money in my account"
- "I haven't been focusing on accs. I do a lot of other types of fraud."

Garrison told a coconspirator that he believed law enforcement would never arrest him for his hacking activity, explaining, "no1 cares ab acc shops. Theyd care if I sold cp on it."

---

[1] In particular, the shops sold access to individual username-password pairs that had been verified to work on the Betting Website. The shops typically adjusted the price at which they sold each account based on how much money was in the account, and the shops also provided instructions as to how to drain money from the account with purchase.

Law enforcement also found an undated picture showing that Goat Shop had sold 225,247 products—meaning stolen accounts—for a total sales revenue of $2,135,150.09.[2] Law enforcement also located cryptocurrency wallets controlled by Garrison that had once held $175,019.11 in cryptocurrency, although those wallets held only de minimis quantities at the time of the search.

II. Procedural History

On February 23, 2023, law enforcement executed a search on Garrison's home in connection with this case and seized his electronic devices.

On May 18, 2023, law enforcement arrested Garrison on a complaint in connection with this case. Through his attorney, Garrison almost immediately began attempting to resolve the case rather than contesting his guilt. After requests for a deferred prosecution agreement and admission to the Young Adult Opportunity Program were denied, he waived indictment and pleaded guilty on November 15, 2023, to an information charging him with one count of conspiracy to commit computer intrusions, in violation of 18 U.S.C. § 371.

III. The Sentencing Guidelines Range

There is no dispute as to the Guidelines Range. The base offense level for the computer intrusion conspiracy is six; 14 levels are added because the loss amount is more than $550,000 but less than $1,500,000; two levels are added because the offense involved 10 or more victims; two levels are subtracted because the defendant has zero criminal history points and meets certain other criteria; and three levels are subtracted because the defendant accepted responsibility for his crime. The defendant has no prior convictions and is in criminal history category I. His resulting Guideline range is 24 to 30 months' imprisonment.

Probation recommends a sentence of one year and a day. The defendant requests a non-custodial sentence. The statutory maximum term of imprisonment is 60 months.

IV. The Appropriate Sentence

A. Applicable Law

While advisory following *United States v. Booker*, 543 U.S. 220 (2005), the Guidelines remain "the starting point and the initial benchmark" for sentencing. *Gall v. United States*, 552 U.S. 38, 49 (2007). That is because the Guidelines are "the product of careful study based on extensive empirical evidence derived from the review of thousands of individual sentencing decisions." *Id.* at 46. For that reason, "in the overwhelming majority of cases, a Guidelines sentence will fall comfortably within the broad range of sentences that would be reasonable in the particular circumstances." *United States v. Fernandez*, 443 F.3d 19, 27 (2d Cir. 2006).

---

[2] Garrison told law enforcement that he only controlled Goat Shop for a brief period of time, and the Government believes that other individuals may well have controlled Goat Shop at other times. The Government is therefore not holding Garrison responsible for all those sales.

In imposing a sentence, the Court must consider seven factors outlined in Title 18, United States Code, Section 3553(a): (1) "the nature and circumstances of the offense and the history and characteristics of the defendant"; (2) the four legitimate purposes of sentencing, as set forth below; (3) "the kinds of sentences available"; (4) the Guidelines range itself; (5) any relevant policy statement by the Sentencing Commission; (6) "the need to avoid unwarranted sentence disparities among defendants"; and (7) "the need to provide restitution to any victims," 18 U.S.C. § 3553(a)(l)–(7). *See Gall,* 552 U.S. at 50 & n.6.

In determining the appropriate sentence, the statute directs judges to "impose a sentence sufficient, but not greater than necessary, to comply with the purposes" of sentencing, which are:

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;
(B) to afford adequate deterrence to criminal conduct;
(C) to protect the public from further crimes of the defendant;
(D) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner.

18 U.S.C. § 3553(a)(2).

B. The Court Should Impose a Sentence of at Least 18 Months

The defendant's crime was extremely serious. The Attack resulted in the compromise of accounts belonging to 60,000 individuals.[3] Each of those individuals in effect had their identities stolen, and were likely subject to some degree of stress and aggravation as a result. The Attack stole $600,000 from those individuals, and the Betting Website's total cost from the Attack was well over a million dollars.

Critically, this was not a one-off crime by the defendant. He engaged in similar credential stuffing attacks for *years*, with an untold number of additional identity theft victims. In his messages, he expressed no remorse at all, and in fact described how much he enjoyed stealing the identities of ordinary people and selling access to those identities online.

Deterrence is a key consideration in this case. The defendant in this case was not deterred by a police visit to his home, and even bragged to law enforcement about his hacking. His messages made clear that he thought he would never be caught or punished for his criminal conduct. The defendant engaged in his credential stuffing attacks and sale of stolen accounts as part of a large network of coconspirators, and that degree of impunity appears to be common in that community. General deterrence is therefore also significant—any sentence should send the message that such a crime is not harmless and will result in serious criminal penalties.

[3] In light of the number of individual victims, the Government has requested permission to notify victims by other means, dkt. 21, and has published that notice online, https://www.justice.gov/usao-sdny/us-v-garrison-23-cr-597-lak.

Were the defendant even slightly older, the Government would almost certainly recommend a sentence within the Guidelines Range of 24 to 30 months. This defendant, however, committed the Attack less than two months after his 18th birthday; has been fully compliant with his bail conditions; and graduated from high school and enrolled in college while on pretrial release. Any sentence should balance the need for serious punishment with the hope that the defendant can get his life on track and become a productive member of society. A sentence of at least 18 months is accordingly sufficient but no more than necessary to serve the purposes of sentencing.

V. Restitution and Forfeiture

The defendant is responsible for a total loss amount of $1,327,061, representing the cost to the Betting Website of making the individual victims whole and otherwise responding to the Attack. The defendant has agreed to pay restitution in that amount to the Betting Website, and an unsigned consent restitution order is attached hereto.

The defendant has also agreed to pay forfeiture in the amount of $175,019.11, which represents the Government's conservative estimate of how much money the defendant earned in connection with his hacking activity generally. The Government has previously submitted a consent preliminary order of forfeiture in the case. Dkt. 20-4.

VI. Conclusion

For the reasons set forth above, the Government respectfully requests that the Court impose a sentence of at least 18 months' imprisonment.

Respectfully submitted,

DAMIAN WILLIAMS
United States Attorney

by: /s/
Kevin Mead
Micah Fergenson
Assistant United States Attorneys
(212) 637-2211/2190

cc: All Counsel of Record (ECF)